(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number : **0 379 333 B1**

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication of patent specification : **12.07.95 Bulletin 95/28**

(51) Int. Cl.[6] : **G07F 7/10**, G07F 7/08

(21) Application number : **90300442.2**

(22) Date of filing : **16.01.90**

(54) Secure data interchange system.

(30) Priority : **17.01.89 CA 588388**

(43) Date of publication of application : **25.07.90 Bulletin 90/30**

(45) Publication of the grant of the patent : **12.07.95 Bulletin 95/28**

(84) Designated Contracting States : **AT BE CH DE DK ES FR GB GR IT LI LU NL SE**

(56) References cited :
EP-A- 0 216 298
EP-A- 0 220 703
EP-A- 0 223 122
EP-A- 0 243 873
CA-A- 1 207 460

(56) References cited :
GB-A- 1 504 196
GB-A- 1 505 715
GB-A- 2 181 582
GB-A- 2 185 937
US-A- 3 702 464
US-A- 4 138 058

(73) Proprietor : **Graves, Marcel Albert**
14008-80 Avenue
Edmonton Alberta T4R 3J7 (US)

(72) Inventor : **Graves, Marcel Albert**
14008-80 Avenue
Edmonton Alberta T4R 3J7 (US)

(74) Representative : **Howick, Nicholas Keith et al**
CARPMAELS & RANSFORD
43 Bloomsbury Square
London WC1A 2RA (GB)

EP 0 379 333 B1

Description

FIELD OF THE INVENTION

This invention relates generally to a system of providing information and services to a population of persons through portable devices which can be used to access any of a number of terminals to make use of the services offered at the said terminals. The system in particular provides for security against unauthorized access. The invention has use in the fields of automatic banking, automatic credit and debit transactions, passport and travel visa verification, health and medical records, security access, licensing and any other like field where fraud may pose a problem.

BACKGROUND OF THE INVENTION

Data transfer systems using portable devices such as cards with some memory capability, for example, a magnetic strip, and terminals to which the portable devices can be connected are well known. Generally they are used to control access to some area or service. Usually the terminals are connected to a central processing unit or computer which controls access and is the ultimate storage facility for the information on the card.

British Patent 1504196 to Moreno describes such a prior art system comprised of a portable device and a peripheral device or terminal which is connected to a central computer. Many of the portable devices referred to as prior art in Moreno used magnetic track memories which could easily be modified or the contents read. Also the memory storage capacity was quite low and the memory was susceptible of accidental modification. This left such systems vulnerable to abuse from fraudulent intervention.

United States Patent 3702464 addressed the problem of lack of memory capacity and volatility by disclosing a portable device containing an integrated circuit memory. The device still suffered from the problem that the memory could be read and the contents extracted or changed. Moreno advanced the art by adding inhibiting means to prevent the transfer of data out of or into prohibited areas of the memory of the portable device. Preferably the portable device contained its own inhibiting means but the inhibiting means could be contained in the peripheral device.

In British Patent 1505715 to Moreno there is disclosed a system for interchanging information which is like those described above, but without the error prone direct connections from the peripheral devices connected to the central computer. The peripheral devices contained a write mechanism which could transfer the information from the portable device to the peripheral device which could in turn write the information on a second portable device. These second portable devices would then be collected on some regular basis and taken to the central computer where the information would be transfered to the central computer's memory.

Canadian Patent 1207460 to Ugon discloses a method and apparatus for authorizing access to a service offered by an authorizing entity. The system comprises a portable card with memory and a microprocessor, and an authorizing entity system capable of communicating with the card and also performing computer program operations. The card and the system have the same algorithm to be executed and each has secret data upon which the algorithms operate to produce a result which can be compared to ensure that proper access is granted. This system is rather complicated and involves an operator at the authorizing entity end.

It is also known to encode a fingerprint on a portable card to verify the identity of the user. UK Patent Application GB 2185937 A of O'Shea et al discloses a credit or similar card which incorporates a computer generated image of the fingerprint of the authorized user. When a transaction is to be verified the user's finger print is scanned by a finger print reader and the result is compared with the information on the card. The user is authorized to have access if the prints match. Such devices are presently commercially available.

EP-A-223122 discloses a secure component authentication system which carries out a "hand shaking" routine. The verification of the terminal, for example, takes place by the card transmitting an encrypted number (X) to the terminal. The terminal decrypts the number (X) using its key K2, to form a number (Y), which is then used as a key to encrypt the terminal key (K2) to form a number (Z). This number (Z) is transmitted to the card, where it is verified at the card that the number (Z) equals the encryption of the encryption key of the card using its number (RN) as the key, thereby to authenticate the terminal.

EP-A-216298 describes a similar authentication system. An IC card, a data memory and a comparator as well as means capable of electrically communicating with the card terminal when the card is loaded thereon are provided. The terminal is verified by first transmitting to the terminal encrypted data which is read out from the data memory in the card. This data is acted on by the terminal and transmitted to the card. The terminal is then verified by the card by comparing this data received to data stored in its data memory. Should there be coincidence of this data received and data in memory, the card advances to the next step of the verification process.

The systems described above suffer from the problem of complexity or they are susceptible to fraudulent and unauthorized access and tampering with the information in the card or the terminal. The present invention provides a highly secure and highly fraudproof system for providing access to services of an authorizing entity.

SUMMARY OF THE INVENTION

According to the invention, there is provided a system for the secure interchange of information according to claim 1.

In the preferred embodiments of the invention, the system comprises a portable device such as a card, a peripheral device such as a terminal, and optionally, a remote host computer in the case of large systems, although it can be seen that the host computer is not necessary for an operational system. These components are connected via some communication medium such as electrical connectors or optics or radio transmission . The terminal contains a microprocessor or some such logic device and memory, a card reading device and a finger print scanner. The card contains a microprocessor or some such logic device and memory, which can be connected to the terminal via electronic or some other means such as optics or radio transmission. The card and terminal each have their own data and programs. Upon insertion of the card into the reader a process of verification is carried out by means of the microprocessors or logic units, the programs and data in the memories. The card verifies that the terminal is valid, the terminal verifies that the card is valid and the user is verified by means of a finger print scan and comparison with finger print data previously recorded in the card. This is not to say that some other form of physical characteristic could not be used such as retinal or DNA scan. Where data is being transmitted between components of the system encoding and decoding is used to further enhance the security of the system.

The system of the invention may be used in a method of preventing unauthorized access wherein, when the said terminal is connected to the said portable device and power is supplied to the said portable device the terminal device queries the portable device to determine if it is a valid portable device, if not the portable device is retained or rejected by the terminal, in turn the portable device queries the terminal to determine if the terminal is a valid terminal, if not the portable device erases its memory and becomes harmless, the terminal in turn scans a physical characteristic of the user and compares that information with stored information on the portable device to determine if that user is authorized to use the portable device and the terminal, if the portable device and terminal are valid and the user is authorized access is allowed to the service, if not the card is retained or rejected; when the power to the terminal is interrupted the terminal programs and data are lost and can only be reloaded by authorized personnel with their access portable devices or from the host computer; encryption is used at the portable device and terminal interface as well as at the terminal and host computer interface.

BRIEF DESCRIPTION OF THE DRAWINGS

In drawings which illustrate embodiments of the inventions,

Figure 1 is a pictorial representation of the basic system components, including an optional host computer

Figure 2 is a flow chart depicting the dialog between the card and the terminal,

Figure 3 is a block diagram illustrating hardware configuration.

DESCRIPTION OF THE PREFERRED EMBODIMENT

The combining of the capability of an intelligent card co-operating with an intelligent terminal, a finger print scanning device, and optionally interfacing with a host computer to ensure maximum possible protection for a card user and a card issuer, is very desirable. In Figure 1 the basic hardware configuration needed to implement such an idea is set out in pictorial form. The host computer system 1 can be a personal computer, mini-computer, mainframe or any suitable computer configuration depending upon the particular application. The host computer system is connected to terminal 3 by suitable linkages such as a telephone line through a modem. It is also possible to utilize other linkages such as radio transmission, or direct cable or optics. Terminal 3 is described as an intelligent terminal and comprises an output device such as a display 5, or a voice synthesizer or other means of communication with the user, a card reader 6 for reading or writing information from or to the card 4. It also contains an input device 8 such as a keyboard or other means of inputting information to the terminal and a finger print scanning device 7 or some other device to obtain physical information about the user.

When a user wishes to utilize a card to gain access to a service from a terminal, the system requires a unique verification procedure to be implemented. Upon insertion of the card into the terminal, the terminal itself

is verified by the card. The card is then verified by the terminal and then the user's finger print which has been digitized into the card at the time of issue is compared with the finger print which is submitted via the finger print scanning device at the time of use. Additional user identification such as a personal identification number can also be included.

If the terminal into which the card is inserted is not a valid terminal the card will erase its memory rendering itself useless to any would-be unauthorized user.

An invalid card will be retained by the terminal and retrieved by authorized personnel. If the finger prints don't match the card is retained, otherwise access is granted to the service offered by the terminal.

Figure 2 is a detailed flow chart depicting the above sequence of verification. In the preferred embodiment the card is an "intelligent card" with its own microprocessor or logic unit, memory, data and programs. In the preferred embodiment it is envisaged that the card will not carry its own power supply but will be connected to the terminal's power supply when the card is inserted. However, it may be preferable in some cases for the card to have its own power supply.

The whole process will start with the card's insertion into the terminal reader.

The verification process, then, shall start on the terminal side by generating a question directed to the card. On the card side, the checkout is accomplished by simply waiting for a certain period of time for the terminal's question. If the question does not arrive, the card will destroy all information in its memory and become useless.

If one assumes that the card and the terminal are the correct ones, the parallel processing of the input question must proceed on both the terminal and card sides. On the terminal side, the checking of the card is achieved similarly to the card's check by waiting for the answer for a certain period of time. If the answer does not arrive, the terminal can withhold the card or reject it. If the answer does arrive it will process it.

The invention can be configured to use different types of cards for different applications. For example:

1) Passport cards
2) Credit cards
3) Security access cards
4) Licence cards
5) Debit cards

Different types of cards would produce different answers to the initial question. This would be the way the terminal recognizes the type of card it is dealing with. If the answer from the card arrives on time, the terminal would sort the answer to the proper application and proceed by checking if the answer is correct. In the negative case, it would, again, withhold or reject the card.

The next stage is the verification process in which identity of the card user is verified. This is done through a process of finger print checkout, in which the terminal transmits a user identification request to the card. The person's finger prints are scanned and compared with the template received from that stored on the card. Again, if any attempt is made to read the data from the card memory before the finger print verification process is completed, the card will destroy its data.

The card will only allow access to its memory after confirmation from the terminal that the user is permitted to use it.

It is unlikely that the whole verification process will take any longer than approximately 25 seconds although the timing is not critical.

It is possible that someone could try to gain access to the data or the software itself by tampering with the terminal. To prevent this, all terminal software could be placed on RAM memory only. This way it would be lost immediately if the power to the terminal is disrupted. Only a licensed technician with his own access portable device would be able to download new software either from his portable device or from the host computer, and bring the terminal up again.

The block diagram of Figure 3 shows the hardware configuration of a preferred embodiment of a simple system comprised of only one terminal. The host computer system 1 is remotely located from the terminal 3. The two are connected by way of a telephone line 2 and modems 10a and 10b. The terminal 3 is composed of a PC-type motherboard 9, which includes a microprocessor or other logic device and memory, an "intelligent card" reader 6, a finger print scanner 7, a custom keyboard 8 and a display 5. The card reader 6 is adapted to receive and communicate with the "intelligent card" 4. The "intelligent card" typically contains a microprocessor or some other logic device and memory. Appropriate software and data are stored in the terminal 3 and in the "intelligent card" 4 to enable the verification procedures represented by the flow chart of Figure 2 to be carried out.

"Intelligent cards" are a unique technology utilizing plastic or some other media in which to embed microprocessor or some such logic unit and memory chips. The cards accordingly have both memory and processing capabilities. Essentially they are pocket sized computer systems with a wide range of application possibilities.

A number of off-the-shelf items can be used in the system. The terminal could use an IBM PC™ mother-

board, a Toshiba™ FZ1318 card reader and an IDENTIX Touchsave™ T5-500 finger print scanner. The "intelligent card" could be a Toshiba TOSMART™ CZ-3000. Typically an IBM PC™ could be used as the host computer but larger more complex systems using many terminals may require a larger computer such as a mainframe.

Interconnections other than telephone lines and modems are possible. For example a security system for a building may have dedicated communication cables connecting the various terminals to the host computer without the use of modems. Also radio and optical interconnections are possible.

Finally to further enhance security an encryption technique could be used to encode data before transmitting between the host computer and the terminal, and decoding upon receipt. Similarly encoding and decoding could be used when reading and writing from and to the "intelligent card".

A number of changes and modifications apparent to one skilled in the art can be made without departing from the invention as defined by the accompanying claims.

Claims

1. A system for the secure interchange of information comprising:
   at least one portable electronic card (4) having a memory for storing program algorithms and data therein including valid terminal verification data and valid user identification request data;
   at least one terminal device (3) adapted to receive and communicate with said portable electronic card;
   said card (4) including:
   means for communicating with said terminal (3);
   means for monitoring, for a predetermined period of time, immediately following insertion of said card (4) in said terminal (3), an output from said terminal (3) for a terminal verification message and being operable to erase said memory when said terminal verification message is not received within said predetermined period of time, and being responsive to said terminal verification message received within said predetermined period of time, by comparing said received terminal verification message to said stored valid terminal verification message and being operable to erase said memory when said received terminal verification message is not valid; and
   means for monitoring, following receipt of a valid terminal verification message, the output from said terminal (3) for a user identification request and being responsive to said user identification request by comparing said received user identification request to said stored valid user identification request and being operable to erase said memory when said user identification request is not valid;
   said terminal device (3) including:
   means for transmitting to said card (4) said terminal verification message, upon insertion of said card (4) in said terminal (3);
   means for monitoring, for a second predetermined period of time a card output for receipt of a card verification message and being operable to reject said card (4) when said card verification message is not received within said second predetermined period of time, and being responsive to said card verification message received within said second predetermined period of time by comparing said received card verification message to a stored valid card verification message, and being operable to reject said card (4) when said received card verification message is invalid;
   means for reading a user identification from said user following receipt of a valid card verification message;
   means for transmitting to said output a user identification request; and
   means for monitoring said card output for receipt of said predetermined user information and being responsive to said predetermined user information for comparing said received predetermined user information to said read user identification, and being operable to reject said card (4) when said predetermined user information is invalid.

2. A system as defined in claim 1, wherein said means for reading is a scanning device (7) for scanning a physical characteristic of said user.

3. A system as defined in claim 2, wherein said physical characteristic is a finger print pattern.

4. A system as defined in any preceding claim, said card including means for transmitting to said terminal, following receipt of valid terminal verification message a card verification message.

Patentansprüche

1. System zum sicheren Informationsaustausch, welches umfaßt:
zumindest eine tragbare elektronische Karte (4) mit einem Speicher zum Speichern darin von Programm-Algorithmen und Daten, welche Überprüfungsdaten eines gültigen Terminals bzw. Datenendstation bzw. Endgliedes und gültige Benutzer-Identifikationsnachfragedaten umfassen;
zumindest eine Terminal-Einrichtung (3), welche angepaßt ist, um die tragbare elektronische Karte aufzunehmen und mit dieser zu kommunizieren;
wobei die Karte (4) umfaßt:
eine Einrichtung zum Kommunizieren mit dem Terminal (3);
eine Einrichtung zum Überwachen bzw. Kontrollieren, während einer vorbestimmten Zeitperiode, welche unmittelbar der Einführung der Karte (4) in das Terminal (3) folgt, einer Ausgabe bzw. eines Ausganges von dem Terminal (3) für eine Terminal-Überprüfungsnachricht, welche betriebsbereit ist zum Löschen des Speichers, wenn die Terminal-Überprüfungsnachricht nicht innerhalb der vorbestimmten Zeitperiode empfangen wird, und welche auf die innerhalb der vorbestimmten Zeitperiode empfangene Terminal-Überprüfungsnachricht anspricht, und zwar durch Vergleichen der empfangenen Terminal-Überprüfungsnachricht mit der gespeicherten gültigen Terminal-Überprüfungsnachricht und welche betriebsbereit ist, um den Speicher zu löschen, wenn die empfangene Terminal-Überprüfungsnachricht nicht gültig ist; und
eine Einrichtung zum Überwachen bzw. Kontrollieren der Ausgabe von dem Terminal (3) für eine Benutzeridentifikationsnachfrage im Anschluß auf den Empfang einer gültigen Terminal-Überprüfungsnachricht bzw. -Information, welche empfindlich ist auf die Benutzeridentifikationsnachfrage durch Vergleichen der empfangenen Benutzeridentifikationsnachfrage mit der gespeicherten gültigen Benutzer-Identifikationsnachfrage und betriebsbereit ist, um den Speicher zu löschen, wenn die Benutzeridentifikationsnachfrage nicht gültig ist;
wobei die Terminal-Einrichtung (3) umfaßt:
eine Einrichtung zum Übertragen an die Karte (4) der Terminal-Überprüfungsnachricht, und zwar beim Einführen der Karte (4) in das Terminal (3);
eine Einrichtung zum Überwachen während einer zweiten vorbestimmten Zeitperiode eines Kartenausganges zum Erhalt einer Kartenüberprüfungsnachricht, welche betriebsbereit ist, um die Karte (4) zurückzuweisen bzw. zu sperren, wenn die Kartenüberprüfungsnachricht nicht innerhalb der zweiten vorbestimmten Zeitperiode empfangen wird und empfindlich ist auf die innerhalb der zweiten vorbestimmten Zeitperiode empfangene Kartenüberprüfungsnachricht durch Vergleichen der empfangenen Kartenüberprüfungsnachricht mit einer gespeicherten gültigen Karten-Überprüfungsnachricht und betriebsbereit ist, um die Karte (4) zurückzuweisen, wenn die empfangene Kartenüberprüfungsnachricht ungültig ist;
eine Einrichtung zum Lesen einer Benutzeridentifikation von dem Benutzer infolge des Erhaltes einer gültigen Karten-Überprüfungsnachricht;
eine Einrichtung zum Übertragen einer Benutzeridentifikationsnachfrage an den Ausgang; und
eine Einrichtung zum Überwachen des Kartenausganges für den Erhalt der vorbestimmten Benutzerinformation, welche empfindlich ist auf die vorbestimmte Benutzerinformation zum Vergleichen der empfangenen vorbestimmten Benutzerinformation mit der gelesenen Benutzeridentifikation und betriebsbereit ist, um die Karte (4) zurückzuweisen, wenn die vorbestimmte Benutzerinformation ungültig ist.

2. System gemäß Anspruch 1, wobei die Einrichtung zum Lesen eine Abtasteinrichtung (7) ist zum Abtasten einer physischen bzw. physikalischen Charakteristik bzw. Eigenschaft des Benutzers.

3. System gemäß Anspruch 2, wobei die physikalische Charakteristik ein Fingerabdruckmuster ist.

4. System gemäß einem der vorangegangenen Ansprüche, wobei die Karte eine Einrichtung umfaßt zum Übertragen einer Kartenüberprüfungsnachricht an das Terminal infolge des Empfanges einer gültigen Terminal-Überprüfungsnachricht.

Revendications

1. Système pour la sécurité d'un échange d'informations comprenant:
au moins une carte électronique portative (4) ayant une mémoire pour y mémoriser des algorithmes de programme et des données incluant des données de vérification de terminal valide et des données de demande d'identification d'utilisateur valide;

au moins un dispositif formant terminal (3) adapté pour recevoir et communiquer avec ladite carte électronique portative;

ladite carte (4) incluant:

des moyens pour communiquer avec ledit terminal (3);

des moyens pour surveiller, pendant une période de temps prédéterminée, immédiatement à la suite d'une insertion de ladite carte (4) dans ledit terminal (3), une sortie provenant dudit terminal (3) et relative à un message de vérification de terminal et pouvant fonctionner de manière à effacer ladite mémoire lorsque ledit message de vérification de terminal n'est pas reçu à l'intérieur de ladite période de temps prédéterminée, et répondant audit message de vérification de terminal reçu à l'intérieur de ladite période de temps prédéterminée, par une comparaison dudit message de vérification de terminal reçu audit message de vérification de terminal valide mémorisé et pouvant fonctionner de manière à effacer ladite mémoire lorsque ledit message de vérification de terminal reçu n'est pas valide; et

des moyens pour surveiller, à la suite de la réception d'un message de vérification de terminal valide, la sortie provenant dudit terminal (3) et relative à une demande d'identification d'utilisateur et répondant à ladite demande d'identification d'utilisateur par une comparaison de ladite demande d'identification d'utilisateur reçue à ladite demande d'identification d'utilisateur valide mémorisée et pouvant fonctionner de manière à effacer ladite mémoire lorsque ladite demande d'identification d'utilisateur n'est pas valide;

ledit dispositif formant terminal (3) incluant:

des moyens pour transmettre à ladite carte (4) ledit message de vérification de terminal, lors de l'insertion de ladite carte (4) dans ledit terminal (3);

des moyens pour surveiller, pendant une seconde période de temps prédéterminée, une sortie de la carte relative à la réception d'un message de vérification de carte et pouvant fonctionner de manière à rejeter ladite carte (4) lorsque ledit message de vérification de carte n'est pas reçu à l'intérieur de ladite seconde période de temps prédéterminée, et répondant audit message de vérification de carte qui est reçu à l'intérieur de ladite seconde période de temps prédéterminée par une comparaison dudit message de vérification de carte reçu à un message de vérification de carte valide mémorisé, et pouvant fonctionner de manière à rejeter ladite carte (4) lorsque ledit message de vérification de carte reçu est invalide;

des moyens pour lire une identification d'utilisateur provenant dudit utilisateur à la suite de la réception d'un message de vérification de carte valide;

des moyens pour transmettre vers ladite sortie une demande d'identification d'utilisateur; et

des moyens pour surveiller ladite sortie de la carte relativement à la réception de ladite information d'utilisateur prédéterminée et répondant à ladite information d'utilisateur prédéterminée pour comparer ladite information d'utilisateur prédéterminée reçue à ladite identification d'utilisateur reçue, et pouvant fonctionner de manière à rejeter ladite carte (4) lorsque ladite information d'utilisateur prédéterminée est invalide.

2. Système selon la revendication 1, dans lequel lesdits moyens pour lire sont constitués par un dispositif de balayage (7) pour balayer une caractéristique physique dudit utilisateur.

3. Système selon la revendication 2, dans lequel ladite caractéristique physique est un motif d'empreinte digitale.

4. Système selon l'une quelconque des revendications précédentes, dans lequel ladite carte inclut des moyens pour transmettre audit terminal, à la suite de la réception d'un message de vérification de terminal valide, un message de vérification de carte.

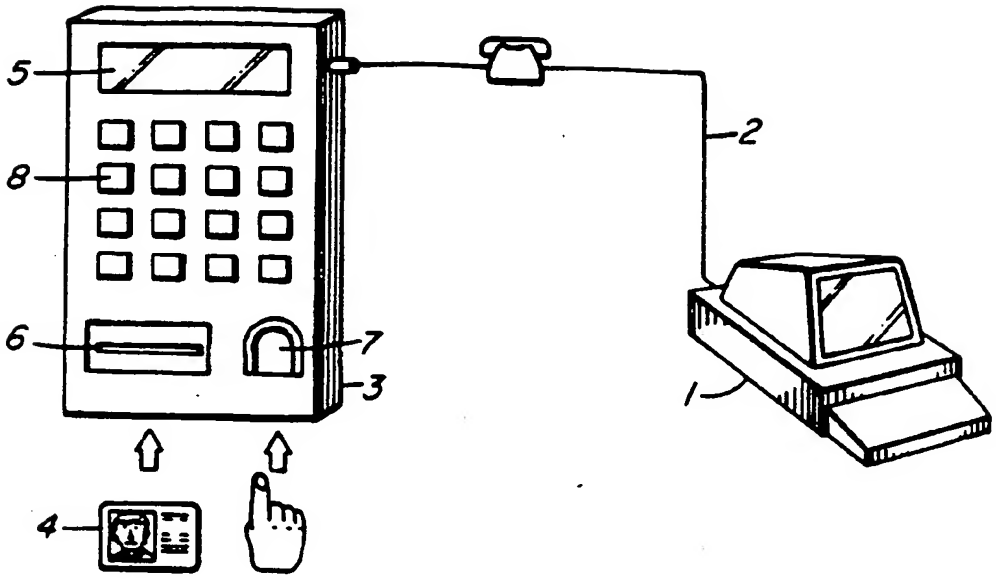
5
8
6
7
3
2
1
4

FIG. 1

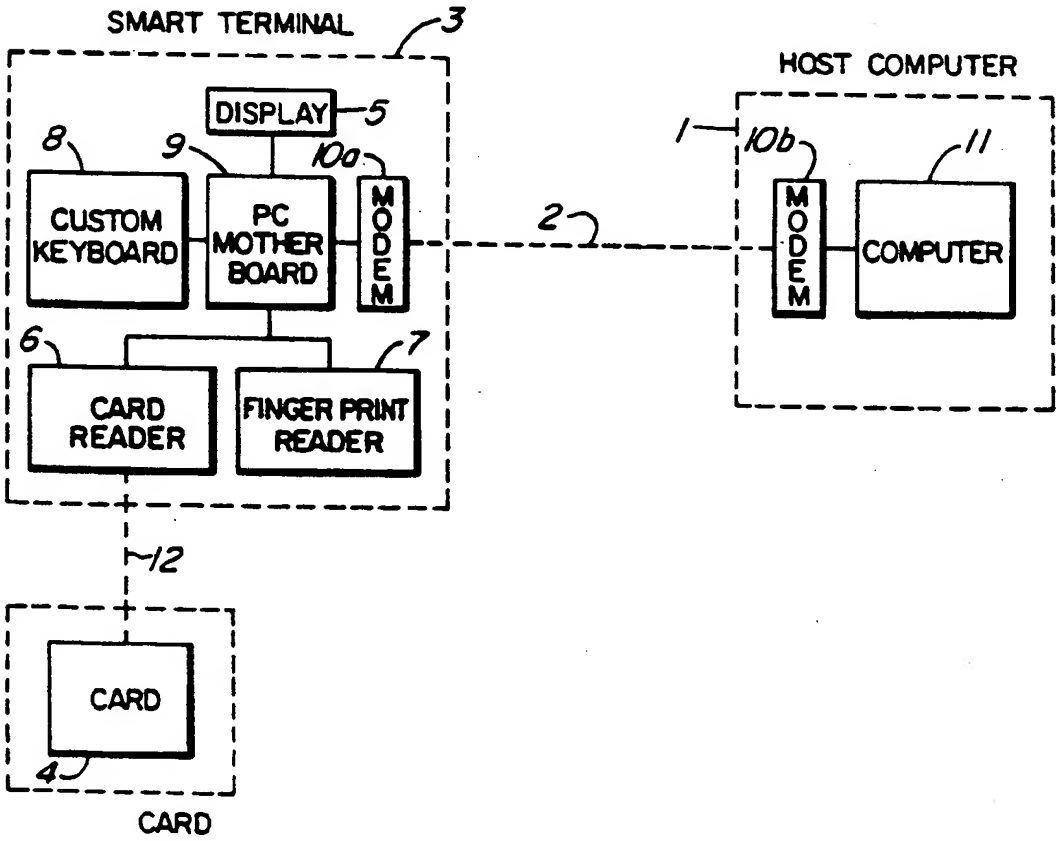
SMART TERMINAL
3
DISPLAY
5
8
9
10a
CUSTOM KEYBOARD
PC MOTHER BOARD
MODEM
2
6
7
CARD READER
FINGER PRINT READER
12
CARD
4
CARD
HOST COMPUTER
1
10b
11
MODEM
COMPUTER

FIG. 3

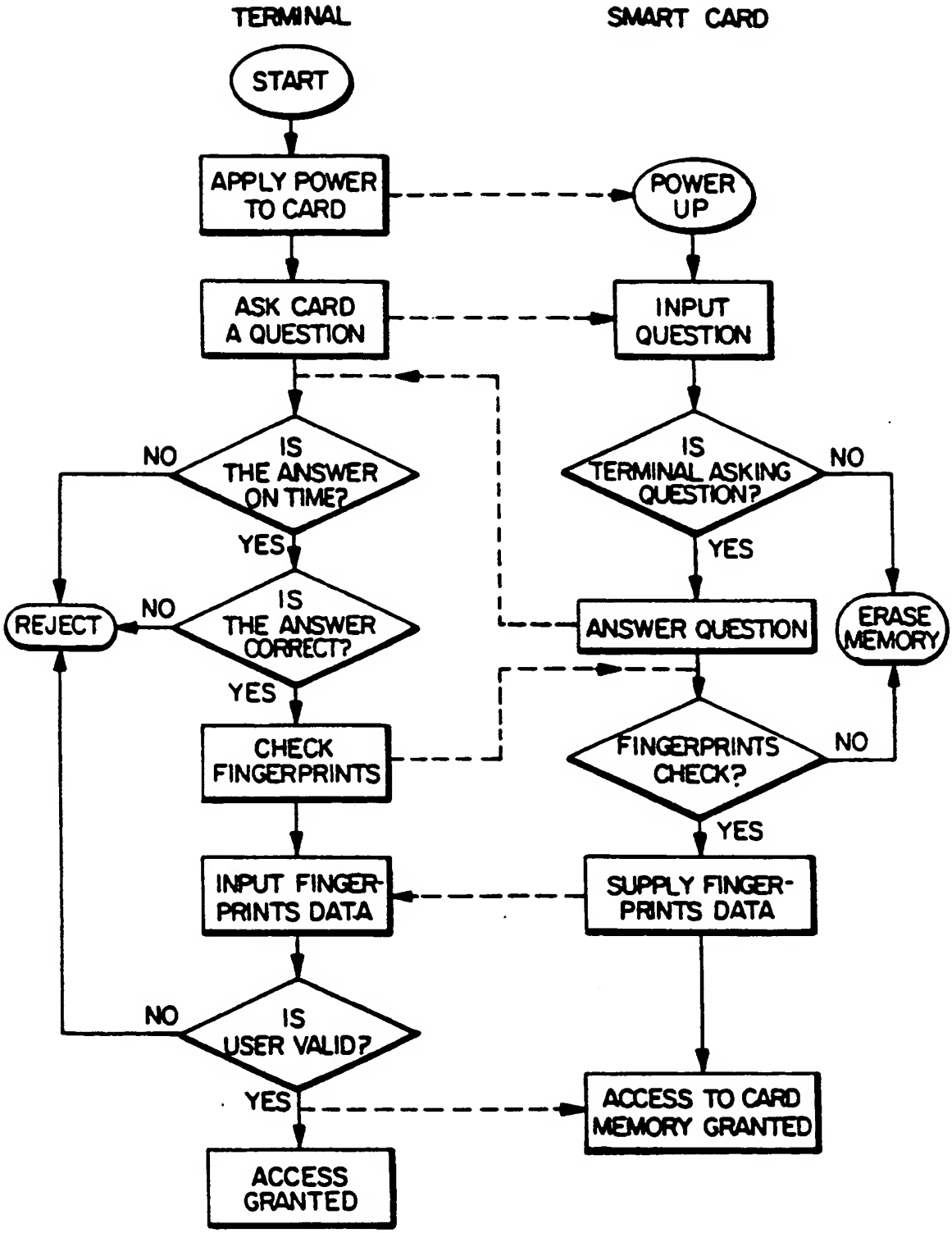
TERMINAL
SMART CARD
START
APPLY POWER TO CARD
POWER UP
ASK CARD A QUESTION
INPUT QUESTION
IS THE ANSWER ON TIME?
NO
YES
IS TERMINAL ASKING QUESTION?
NO
YES
REJECT
NO
IS THE ANSWER CORRECT?
YES
ANSWER QUESTION
ERASE MEMORY
CHECK FINGERPRINTS
FINGERPRINTS CHECK?
NO
YES
INPUT FINGER-PRINTS DATA
SUPPLY FINGER-PRINTS DATA
NO
IS USER VALID?
YES
ACCESS TO CARD MEMORY GRANTED
ACCESS GRANTED

FIG. 2